IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN MARIANA ISLANDS

IN THE MATTER OF THE SEARCH OF

Bonifacio SAGANA residence, Lot ID #011 H 24, Chalan Kanoa Village, Saipan, located two (2) houses South of Francisco Street, on the Northeast corner of Nicolasa Avenue

Miscellaneous Case No. MC21 00007

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, David West, being first duly sworn, do hereby state as follows:

I. INTRODUCTION

1. I am a Special Agent (SA) employed with U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) and have so been employed since September 2018. I am assigned to the HSI Saipan office in the Commonwealth of the Northern Mariana Islands (CNMI). Prior to joining HSI, I worked as a Patrol Agent with the United States Border Patrol for over ten years.

2. I have attended and graduated from the Border Patrol Academy in 2008, as well as the Criminal Investigator Training Program, and the HSI Special Agent Training Academy held at the Federal Law Enforcement Training Center in Glynco, Georgia. I have received extensive classroom and on the job training in the areas of general law enforcement, criminal investigative techniques, interviews and interrogations, general and electronic surveillance, criminal and constitutional law covering federal search and seizure statutes, the execution of search warrants, and interviewing both suspect and victims of crimes, among others. Additionally, during my law enforcement career, I have received training in the investigation and enforcement of both

administrative and criminal statutes related to the U.S. Immigration and Nationality Act (INA).

3. My duties as an HSI SA include investigating violations of Federal laws pursuant to Titles 8, 18, 19, 21, 31 and others. These Titles collectively encompass a wide range of Federal statues such as harboring aliens, smuggling, financial and commercial investigations, materially false statements made to a federal agency, immigration benefit and/or identity fraud, passport application fraud, bank fraud, mail fraud, wire fraud, narcotics and contraband smuggling and distribution, conspiracies to defraud the United States and other violations.

4. As a law enforcement officer, I have been involved in the use of physical surveillance of individuals or premises, review and inspection of official documents and other records, and other investigative techniques. I have controlled, directly assisted, and participated in the execution of numerous federal and State arrest and search warrants, searches of people, residences, and property of people, suspected of criminal violations of law; and have interviewed numerous individuals who were suspected of, or admitted to violations of law.

5. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing a search of the premises at Lot ID #011-H-24, Chalan Kanoa Village, Saipan, MP 96950, further described in Attachment A.

6. I request this warrant to search the aforementioned premises and seize any evidence of violations of 18 U.S.C. § 1546, Fraud and Misuse of Visas, Permits, and Other Documents. Evidence to be searched for and seized during the search is more particularly described in the following paragraphs and in Attachment B. Title 18 U.S.C. § 1546(a) makes it a Federal crime to knowingly forge, counterfeit, alter or falsely make any immigrant or nonimmigrant visa, permit, border crossing card, alien registration receipt card or documents for entry or as evidence of authorized stay in the United States. According to Ninth Circuit Model

Jury Instruction No. 8.132, the pertinent elements of a violation of Title 18 U.S.C. § 1546(a) are as follows:

a. First, the defendant forged, counterfeited, altered or falsely make an immigrant or nonimmigrant visa, permit, border crossing card, alien registration receipt card or other document prescribed by statute or regulation for entry into or as evidence of authorized stay or employment in the United States;

b. Second, the defendant acted knowingly.

7. The facts set forth herein are based on my direct involvement in this investigation, on interviews of individuals identified in the course of this investigation, my conversations with law enforcement officers having direct or hearsay knowledge of pertinent facts, my review of any official documents and records generated and maintained by various local and federal agencies, and information gained through my own training and experience. I have also discussed the facts of this investigation with other law enforcement officials within HSI who have more extensive experience in criminal investigations regarding similar offenses than I, and whom shared with me the substance of their experiences in conducting investigations of this nature. All of the statements and information contained in this affidavit are true and correct to the best of my knowledge and belief.

8. Based on my training, experience, and prior discussions with other experienced law enforcement officials within HSI, I am aware that it is generally common practice for persons involved in the preparation, production, manufacturing and the selling and distributing of fraudulent documents and applications, to conduct illegal activities at their residence. Such operations create and sell documents and supporting applications with manufactured data, utilizing computers, printers, scanners, templates for fraudulent documents, templates for fraudulent applications, and other items. In addition, such operations have evidence of correspondence to and from their clients, such as letters, envelopes, copies of supporting documents, and copies of

legitimate and fraudulent documents and applications. Many persons involved in the manufacture of and sale of counterfeit documents and fraudulent applications utilize this business as their primary source of income and often receive payments from their clients in the form of cash.

9. Persons involved in the preparation, production, manufacturing, selling and distributing of fraudulent documents and applications do business with customers in-person, by mail, by internet, as well as telephonically, and would typically retain records relating to their illegal business activities where they would be readily available, such as at their residence, in their vehicles or on their person. These records include correspondence, notes, daily planners, business and financial transaction records such as ledgers, journals, spreadsheets, receipts, phones and address books, customer lists, notes, pay/owe slips, receipt books, bank statements for personal and business checking and savings accounts, deposit and withdrawal slips, canceled checks, check registers, money order receipts, cashier's checks, investment documents, loan agreements, and wire transfer documents, immigration documents, driver's license and immigration applications, document editing computer programs and software, and correspondence to include electronic mail (e-mail), social media applications, and short messaging service (SMS) texts.

10. It has been my experience and the experience of other agents with whom I have spoken that persons involved in these type of schemes commonly generate or maintain these records in electronic format, using various types of electronic devices including personal desktop computers, laptop computers, personal digital assistants, tablet devices, cellular phones, smartphones, external hard disk drives, memory sticks, and compact discs or DVDs. I am also aware that they are able to convert paper records into electronic format through existing software available to the public. Furthermore, these electronic records can be transmitted via the Internet using electronic devices such as personal desktop computers, laptop computers, personal digital

assistants, tablet devices, and smartphones.

11. In addition, other evidence relating to obtaining, transferring, secreting or spending various sums of money made from the manufacturing and sale of counterfeit documents and fraudulent applications and related criminal activity would commonly be found at the residence of the person. Such persons are often in personal possession of the fruits of their crimes, such as currency, checks, cashier's checks, and money orders. Such persons then use those fruits to pay personal obligations such as mortgages, rent, vehicle loans, personal loans, credit card debts, utility bills, medical bills, and taxes. Records of these personal expenditures, which include cash receipts, personal bank records, invoices, credit card statements, billing statements, installment purchase agreements, rental contracts, and other financial instruments, would usually be maintained at the a residence of an individual who does not maintain a work space at a business location.

12. It is my experience and the experience of other agents with whom I have spoken that persons and organizations involved in the manufacture of and sale of counterfeit documents and fraudulent applications take steps to conceal their income, so as to avoid detection of their illegal activities and to avoid tax payments. It is common for such persons to register their assets, such as bank accounts, vehicles, homes, and real estate in the names of relatives or associates. It is also common for such persons and organizations to set up sham or "dummy corporations" or other business entities through which funds are moved in order to conceal their illicit income and to avoid tax payments.

13. Because this affidavit is being submitted for the limited purpose of securing a warrant to search the described premises, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence of violations of 18 U.S.C. § 1546, are located

within the aforementioned premises. Facts not set forth or incorporated herein are not being relied upon in reaching my conclusion that a search warrant should be issued.

II. CNMI BUREAU OF MOTOR VEHICLES (BMV) DRIVER'S LICENSE REQUIREMENTS

14. Prior to Federalization in 2009 BMV with the intent of issuing a state identification document compliant with U.S. REAL ID Act of 2005 guidelines, CNMI BMV has voluntarily instituted policies and requirements governing the issuance and/or renewal of driver's licenses to non-US citizen residents of the CNMI. Among these requirements is documentary proof of lawful U.S. immigration status in the CNMI at the time of driver's license application or renewal. Other requirements include completion of a CNMI BMV driver's license application form, proof of payment of associated driver's license initial or renewal fees, a CNMI Superior Court traffic clearance and a valid passport.

15. Types of immigration-related documents accepted by CNMI BMV officials as proof of valid stay in the CNMI include I-551 U.S. Permanent Resident ("Green") Cards, I-94 Arrival/Departure Cards typically issued to recipients of Parole of Place (PIP), I-797 Notice of Action receipts for CW-1 nonimmigrant CNMI-only transitional workers, U.S. immigrant and nonimmigrant visas, and valid CNMI-only conditional parole tourist/visitor endorsements stamped by U.S. Customs and Border Protection. CNMI BMV officials may also accept photocopies of these documents. Each of the aforementioned documents are U.S. Department of Homeland Security-issued documents prescribed for entry into the U.S., or evidence of authorized stay and/or employment in the U.S.

III. SUMMARY OF INVESTIGATION

16. In September 2014, HSI Saipan personnel received information that Bonifacio

Vitug SAGANA (SAGANA) was allegedly assisting foreign nationals in the CNMI with obtaining new or renewal of CNMI driver's licenses at the CNMI BMV. These foreign nationals assisted by SAGANA had no valid U.S. immigration status and were therefore unable to lawfully obtain or renew their driver's license because of CNMI regulations requiring proof of lawful stay in the CNMI as part of the licensing or renewal process. These individuals allegedly paid SAGANA $150 US Dollars or more for his assistance, which resulted in the individuals receiving a new or renewed CNMI driver's license.

17. HSI Saipan personnel identified several individuals that were assisted by SAGANA and reviewed their driver's license applications. HSI personnel found that the I-94 documents submitted to the CNMI BMV as evidence of the applicants' lawful status were, in fact, fraudulent.

IV. STATEMENT OF PROBABLE CAUSE

18. In June 2019, Homeland Security Investigations (HSI) Special Agent (SA) Mike Lansangan reviewed [redacted] Castro's alien file, AFN: [redacted], a citizen of the Republic of the Philippines, and a digital copy of his CNMI driver's license renewal application. This CNMI application packet was part of several CNMI BMV records previously obtained by HSI Taskforce Officer (TFO) Jesse Dubrall.

19. While reviewing Castro's alien file, SA Lansangan noted that Castro previously submitted correspondence to United States Citizenship and Immigration Services (USCIS) in Guam on August 9, 2012 and December 14, 2012. In his letters, Castro requested for humanitarian Parole in Place (PIP) and indicated that he had been terminated from his job at GPPC Construction on Saipan. SA Lansangan also found correspondence from USCIS Guam dated March 4, 2013, denying Castro's PIP requests on the basis that he was previously granted CW-1 nonimmigrant status and was therefore ineligible for PIP status.

20. On June 11, 2019, TFO Dubrall and SA Lansangan met Castro at the HSI office. This meeting was previously arranged telephonically by SA Lansangan. Prior to the interview, Castro was advised of his rights. After waiving his rights, Castro admitted to applying for a CNMI driver's license, which was renewed in 2015. Since Castro did not have any valid immigration status to reside in the CNMI, he asked a friend who put him in touch with a Filipino man, subsequently identified as SAGANA, to help renew his CNMI driver's license.

21. Castro recalled meeting SAGANA in San Antonio village. SAGANA told Castro that if Castro wanted to renew his driver's license, he (SAGANA) could help but Castro would have to pay. SAGANA did not tell Castro how he was going to help him renew his driver's license. Castro agreed and provided SAGANA with his expired CNMI driver's license.

22. The next day, SAGANA drove Castro to the police station. Castro recalled that he paid the license renewal fee and traffic clearance at the CNMI court building. They then went to the police station to apply for Castro's driver's license. Castro completed the driver's license application and provided it to SAGANA. As Castro waited, SAGANA did the processing at the window. Later, Castro was called to take his picture and was issued a CNMI driver's license. On the way to SAGANA's vehicle, Castro paid him $200 US Dollars in cash for helping him to get his driver's license.

23. SA Lansangan presented Castro with a copy of his 2015 CNMI driver's license application and asked that he review the document. After reviewing the application, Castro confirmed his information, handwriting and signature on the form. SA Lansangan showed Castro a copy of the I-94 immigration document, bearing number: [redacted], that had his biographical information. This I-94 immigration document was submitted with his CNMI driver's license application. Castro did not recognize this document and did not know how it became part of his

CNMI driver's license application. Castro confirmed that he was never granted PIP status by USCIS.

24. Castro was shown a photo line-up of six males with similar features and asked if he recognized anyone. After reviewing the images, Castro identified an individual that looked like the person that assisted him with renewing his CNMI driver's license in 2015. The individual identified by Castro in the photo line-up was SAGANA.

25. On June 17, 2019, TFO Dubrall and SA Lansangan met Bernardita Zata at the HSI office. This meeting was previously arranged by SA Lansangan. After being advised of her rights, Zata agreed to an interview. Zata stated that she is a citizen of the Republic of the Philippines and has been in the CNMI since 1994 and had previously been issued a CW-1 visa that expired in 2014.

26. According to Zata, she had heard about a Filipino man named "Boni," subsequently identified as SAGANA, that can help Filipinos with no status or CW-1s get a CNMI driver's license. Zata stated that many Filipinos know that SAGANA can assist with getting a CNMI driver's license. Zata's driver's license was about to expire, but she could not renew it because she did not have immigration status. Zata does not personally know SAGANA but remembered him from when she was attending a meeting a few years ago.

27. Sometime in 2017, Zata saw SAGANA in a store and asked if he could help her renew her license even though she did not have any CW-1 status. SAGANA replied yes and told Zata to prepare her money. SAGANA also provided Zata with his telephone number. Zata does not remember the amount SAGANA told her, but she believed it was between $150 to $250 US Dollars.

28. A few days later, Zata called SAGANA and made plans to renew her driver's license. On the day Zata renewed her driver's license, she met SAGANA at the CNMI court building and paid him between $150 to $200 US Dollars. Zata also provided SAGANA with her expired driver's license. While SAGANA paid for the driver's license fees at the CNMI court building, Zata waited for him at the BMV office. After 5 to 15 minutes, SAGANA arrived at the BMV office. Zata recalled that he was carrying something like a purse. Zata does not recall if SAGANA or someone else filled out the application form but surmised that she must have given them the information. SAGANA took care of the processing at the window. After, Zata was called to take her picture and was then issued a CNMI driver's license.

29. SA Lansangan showed Zata a copy of her 2017 driver's license application. Zata confirmed that she signed this document. SA Lansangan then showed Zata a copy of the I-94 immigration document, bearing number: [redacted], that was associated with her driver's license application. Zata didn't recognize this document and doesn't know how this immigration document were submitted with her driver's license application.

30. Zata was shown a photo line-up of six males with similar features and asked if she recognized anyone. After reviewing the images, Zata identified SAGANA and said this is the same person that had assisted with her driver's license renewal.

31. On September 11, 2019, Margarito Villafuerte was interviewed by TFO Dubrall and HSI TFO Raymond Cepeda at the HSI office. Prior to the interview, Villafuerte was advised of his rights, which he waived. Villafuerte is a citizen of the Republic of the Philippines and has been in the CNMI since 2009.

32. According to Villafuerte, in 2017 he was aware that his CNMI driver's license was about to expire and knew he could not renew it on his own because he did not have any immigration

status. Villafuerte stated that he was able to renew his CNMI driver's license with the help of SAGANA. The day prior to his driver's license expiring, Villafuerte called SAGANA and told him that he needed to renew his driver's license and that he did not have any CW-1 or Employment Authorization Document (EAD). SAGANA told Villafuerte that he could help renew his driver's license even if he did not have a CW-1 or EAD, but he (Villafuerte) would have to pay SAGANA $250.00 US Dollars.

33. After Villafuerte agreed, SAGANA met him the next day outside of the BMV office and paid him $250.00 US Dollars in cash. Villafuerte also provided SAGANA with his expired driver's license and Social Security Card. Villafuerte recalled that SAGANA paid for the driver's license fees and handed Villafuerte's driver's license application to someone at the BMV window. A short time later, Villafuerte was called to take his picture. Outside of the BMV, SAGANA provided Villafuerte with his renewed CNMI driver's license.

34. TFO Dubrall showed Villafuerte a copy of his 2017 CNMI driver's license application. Villafuerte reviewed his application and stated that he does not recognize the handwriting but that it did contain his signature. Villafuerte was also shown a copy of the I-94 immigration document, bearing number: [redacted], containing his name and date of birth. Upon reviewing it, Villafuerte stated he does not recognize this form and does not know what it is. Villafuerte does not know how this I-94 immigration document was submitted with his application. Furthermore, Villafuerte stated that he has never received this document from USCIS.

35. On June 12, 2019, HSI interviewed CNMI BMV employee Joselyn Cabrera. Cabrera stated for the past six years she has worked at the BMV office and has regularly seen a Filipino man named, "Bonnie or Bo" bringing foreign nationals to the BMV office. Cabrera identified Bonnie or Bo as SAGANA from a photo lineup. Cabrera stated that SAGANA helps

these foreign nationals with new and renewal of driver's license applications. Cabrera has heard from other BMV staff members that SAGANA gets paid to help his customers at the BMV.

36. According to Cabrera, SAGANA usually comes to the BMV office and approaches the counter while his customer sits down. The applicant's forms, paperwork, and documents are prepared and ready when SAGANA and the applicant come in. SAGANA is the person who interacts with the BMV staff at the window.

37. Cabrera recalled that SAGANA always comes to the BMV office carrying a binder. SAGANA usually retrieves the applicant's paperwork from the binder and submits the paperwork to the BMV staff. Cabrera does not usually interact with SAGANA at the front window or conduct the initial screening of the application packets. Cabrera does review the documents submitted by SAGANA on behalf of the applicants. Cabrera has observed that the majority of SAGANA's customers are Filipinos, but he also sometimes brings in and assists Chinese or Bangladeshi people. Cabrera has also observed that most of the applicants brought in by SAGANA present photocopies of an I-94 document as their proof of valid US immigration status.

38. In October 2019, Resident Agent in Charge Mark Yamanaka conducted a search with DHS databases on the I-94 numbers [redacted]. The search revealed no records of these I-94 immigration documents and the I-94's to be fraudulent.

39. In October 2020, and February 2021, I interviewed CNMI Deputy Marshal (DM) Eric Esteves. DM Esteves stated that he is familiar with SAGANA and has observed him on numerous occasions at the CNMI courthouse going to the clerk and cashier's office with a stack of documents. The last two times, during October 2020, DM Esteves had seen SAGANA at the CNMI courthouse holding multiple driver's license applications.

40. In the past, DM Esteves had asked SAGANA what he did for work. SAGANA told DM Esteves that he "runs papers." DM Esteves believed running papers meant document handling, to include prepare and deliver forms and documents for people and companies. DM Esteves believed SAGANA may have worked for a manpower company, a car dealer or an insurance company due to seeing him with driver's license applications on multiple occasions.

41. In October 2020, I spoke with Immigration and Customs Enforcement, Deportation Officer (DO) Sean White who informed me that he knew SAGANA and where he was living. While conducting official duties, DO White observed SAGANA exiting a house next door to where DO White was working. DO White spoke with SAGANA in the village of Chalan Kanoa. During their conversation, SAGANA informed DO White that he lived at the house next door with his children. As described further in Attachment A, the house (PREMISES), is a white one-story concrete home, with grey roof trim, and three (3) carports. It is located two (2) houses South of Francisco Street, on the North East corner of Nicolasa Avenue, on Lot #011 H 24, in Chalan Kanoa Village, Saipan.

V. COMPUTERS, ELECTRONIC STORAGE AND FORENSIC ANALYSIS

42. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

43. *Probable cause*. I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

44. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

45. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

46. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

47. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or

application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

48. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

49. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crime described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on any such devices found because:

50. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

51. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

52. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

53. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

54. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

55. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded

on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

56. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

57. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

58. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

59. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying

storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

60. SAGANA may conduct legitimate business beyond the scope of that requested in the search warrant. The seizure of SAGANA's computers may limit its ability to conduct its legitimate business. As with any search warrant, Affiant expects that this warrant will be executed reasonably. Reasonable execution will likely involve conducting an investigation on the scene of what computers, or storage media, must be seized or copied, and what computers or storage media need not be seized or copied. Where appropriate, officers will copy data, rather than physically seize computers, to reduce the extent of disruption. If SAGANA requests, the agents will, to the extent practicable, attempt to provide SAGANA with copies of data that may be necessary or important to the continuing function of any legitimate business. If, after inspecting the computers, it is determined that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the government will return it.

61. Computers or other devices that are seized will be retained by the government for not longer than 60 days, unless that time period is extended by the Court for good cause shown. Drives or devices that are imaged by the government will be returned to the owner within that time period, unless the property is forfeitable as contraband, fruits or instrumentalities of the crime, or if the government is otherwise permitted to retain the property by law. If upon initial review, the government determines that the items seized contain data or information that is

outside the scope of this warrant, the government will seal that data or information and will not access it except upon issuance of an additional warrant or order of the Court.

VI. CONCLUSION

62. Based on the facts as set forth in this affidavit, I believe there is probable cause for a search warrant authorizing the search of the premises as described in Attachment A, to seek the documents and other items described in Attachment B, under violations of 18 U.S.C. § 1546, Fraud and Misuse of Visas, Permits, and Other Documents.

63. I have shown this affidavit and the accompanying search warrant application to Assistant United States Attorney Eric O'Malley, and he informs me that they are in proper form.

Respectfully submitted,

David West, Special Agent
Homeland Security Investigations

Subscribed and sworn to before me on March 1, 2021.

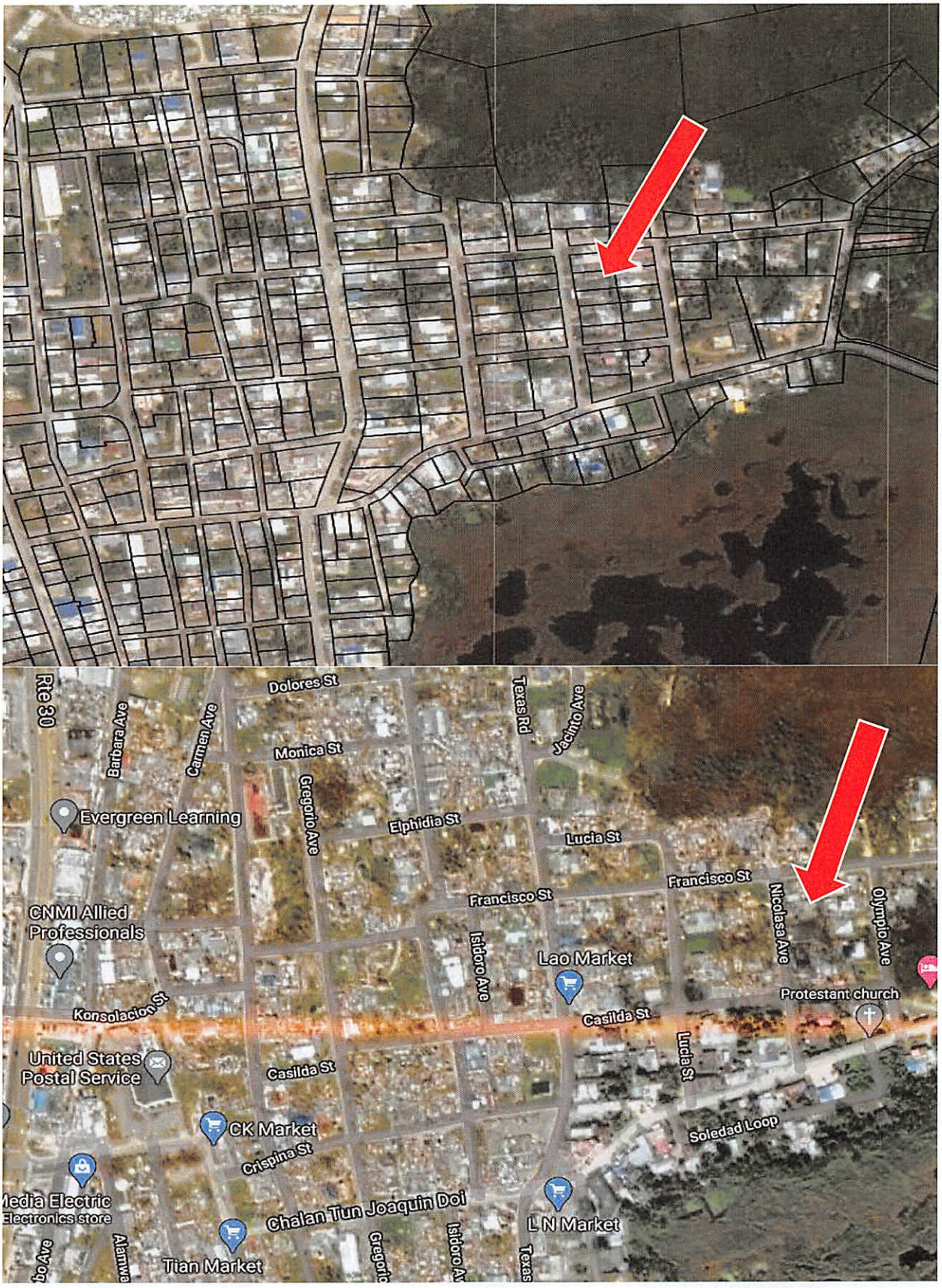
CHIEF JUDGE RAMONA V. MANGLONA
District Court of the Northern Mariana Islands

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

Lot ID #011 H 24, Chalan Kanoa Village, Saipan, MP 96950, Commonwealth of the Northern Mariana Islands (CNMI).

The property to be searched is a West-facing, single story, white concrete with grey roof trim, residential dwelling with three carports. The residence is located in the village of Chalan Kanoa, two (2) houses South of Francisco Street, on the Northeast corner of Nicolasa Avenue (see photographs below) on Lot #011 H 24, Chalan Kanoa Village, Saipan.


Rte 30
Barbara Ave
Carmen Ave
Dolores St
Monica St
Gregorio Ave
Texas Rd
Jacinto Ave
Evergreen Learning
Elphidia St
Lucia St
Francisco St
Francisco St
Nicolasa Ave
Olympio Ave
CNMI Allied Professionals
Isidoro Ave
Lao Market
Protestant church
Konsolacion St
Casilda St
Lucia St
United States Postal Service
Casilda St
CK Market
Soledad Loop
Crispina St
Chalan Tun Joaquin Doi
L N Market
Tian Market

ATTACHMENT B

ITEMS TO BE SEARCHED AND SEIZED

All records relating to violations of 18 U.S. Code§ 1546 Fraud and Misuse of Visas, to fraudulently obtain a CNMI driver's license, specifically those violations occurring on or after January 1, 2016, described in the supporting Affidavit, including but not limited to:

1. Any and all documents and records related to immigration documents, specifically I-94 Arrival and Departure Records, driver's licenses, driver's license applications, CNMI Superior Court Documents, traffic reports, passports, social security cards, travel documents, visas or proof of citizenship or nationality; to include any photographic such as pictures and photocopies.

2. Any and all correspondence and communication records between SAGANA and any past or present client or customer, person or business, including (but not limited to) letters, faxes, emails, mail, memorandums, invoices, contracts, local and long-distancing phone records, texts, SMS messages, names, addresses, telephone numbers, business cards, photographs and any other identifying records and documents, regarding immigration documents or driver's licenses.

3. Books, records, documents, notes, correspondence, communications, receipts, photos, and any other papers relating to a scheme to use counterfeit immigration documents to fraudulently obtain driver's license, including (but not limited to) papers associated with CNMI Bureau of Motor Vehicles.

4. Machines, instruments, equipment, and any indicia of other items that can be used to alter, modify, produce, or create documents or falsify records.

5. Any paper records including travel records, indicia of occupancy, residency and or ownership of the premises, telephone bills, mortgage, deeds and lien records, cancelled mail, bank statements, address and or telephone notebooks, papers, credit cards and bills, wire transfers, money order and cashier check receipts, pass books, check books, bank books, ledgers, diaries, journals and any other items evidencing the obtaining, secreting, transfer, concealment and or expenditure of money.

6. Any and all financial documents pertaining to the unlawful manufacturing of counterfeit documents and document fraud or that constitute the proceeds of or disposition of monies. Any and all bookkeeping records and other financial records, bank statements, other bank records, letters of credit, money orders, cashiers' checks, passbooks, canceled checks, certificates of deposit, loan records, customer account information, income and expense summaries, cash disbursement journals, financial statements, federal and state income tax returns, computer and software records containing financial data and information related to the receipt and other disposition of income and related financial information pertaining to the purchase, lease, sale or other disposition of real or personal property.

7. United States currency, securities, precious metals, jewelry, automobile titles, financial instruments including stocks and bonds in amounts indicative of the proceeds of immigration document fraud, and other items of value and/or proceeds of such related activities, as well as access to locked safes and locked storage containers on the premises and curtilage.

8. Any and all other evidence, fruits, and instrumentalities of the above listed crimes.

For any computer, electronic computing device, or storage medium whose seizure is otherwise authorized by this warrant, and any computer, electronic computing device, or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter "COMPUTER" and "DEVICE"):

1. Evidence of who used, owned, or controlled the COMPUTER or DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat" or other instant messaging logs, photographs, and correspondence;

2. Evidence of software that would allow others to control the COMPUTER or DEVICE, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

3. Evidence of the lack of such malicious software;

4. Evidence of the attachment to the COMPUTER or DEVICE of other storage devices or similar containers for electronic evidence;

5. Evidence of counter-forensic programs, and associated data, that are designed to eliminate data from the COMPUTER or DEVICE;

6. Evidence of the dates, times, and duration the COMPUTER or DEVICE was used;

7. Passwords, encryption codes or keys, and other access devices that may be necessary to access the COMPUTER or DEVICE;

8. Documentation and manuals that may be necessary to access the COMPUTER or DEVICE, or to conduct a forensic examination of the COMPUTER or DEVICE;

9. Records of or information about Internet Protocol addresses used or accessed by the COMPUTER or DEVICE;

10. Records of or information about the COMPUTER or DEVICE's Internet access and activity, including firewall logs, caches, browser history and cookies; "bookmarked" or saved web pages, search terms that a user entered into any Internet search engine, and records of any user-inputted web addresses; and

11. Contextual information necessary to understand the evidence described in this attachment.

As used above:

1. The terms "records" and "information" includes all forms of creation or storage, including any form of computer, electronic computing device, or electronic storage (such as hard disk drives or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies);

2. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptop computers, tablets, mobile phones, smart phones, server computers, and network hardware (including passwords) necessary to ensure the reliable analysis and retrieval of the foregoing electronic documents and tangible objects by a qualified expert; and

3. The term "storage medium" includes any physical object upon which computer data can be recorded or stored. Examples include any electrical, electronic or magnetic form (such as any information on an electronic or magnetic storage device, including floppy disks, hard disks, zip disks, CD-ROM, optical disks, backup tapes, printer buffers, smart cards, USB type storage drives, other flash memory drives, memory calculators, pagers, printouts or readouts from any magnetic storage device or optical media); internal and peripheral storage devices, transistor like binary devices, scanners, keyboards, printers, plotters, video display monitors, modems, cables, connections and recording equipment, RAM, acoustic couplers, automatic dialers, speed dialers, prepaid telephone calling cards, electronic tone generating devices, landline telephones with memory dial or other information storage capability, satellite telephones.